UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,004	12/21/2001	Robert R. Gilman	401043-A-01-US	2388

24283	7590	10/19/2006	

PATTON BOGGS
1660 LINCOLN ST
SUITE 2050
DENVER, CO 80264

· EXAMINER
SZYMANSKI, THOMAS M

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

MAILED

OCT 19 2006

Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/028,004
Filing Date: December 21, 2001
Appellant(s): GILMAN ET AL.

James M. Graziano
Reg. No. 28,300
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/22/2006 appealing from the Office action

mailed 2/28/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Chang et al U.S. Patent No. 5,724,425

Ho et al U.S. Patent Publication No. 2002/0073325

Horstmann U.S. Patent No. 6,044,469

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-5, 10-14 and 16-17 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Chang et al U.S. Patent No. 5,724,425, and further in view of Ho et al

U.S. Patent Publication No. 2002/0073325.

Chang et al.("Chang") has taught the method of authentication as in the claimed

invention, but fails to teach the implementation of an owner key that is unique to the

given computer system.

Ho et al ("Ho"), however, teaches the use of a key specific to the individual

computer system for the purposes of license integrity.

It is desirable to maintain the authenticity of a software program from malicious

attack by worms, viruses and other programs or individuals that have the common intent

of harming a host system. Such programs are known to often compromise critical

information of such a system and cause additional damage. As taught by Chang et al

such attacks are avoidable by the implementation of a signature system that is

composed of a message digest to confirm the integrity of software. Ho teaches that a

greater level of security may be obtained by the implementation of a unique key

signature of a system so as to prevent that particular license from being compromised

(Ho paragraphs 4-12, Chang Col 1 line 50-Col 3 line 13)

It would have been obvious to one of ordinary skill in the art at the time of the

applicant's invention to combine the system of Ho into that of Chang for the advantages

as stated above. The combination of two such systems includes the unique identifier of the Ho system implemented for the key system of Chang while maintaining the ability of Chang to protect the integrity of software the system is expanded to include the feature of uniquely defining the entitlement of the license to the specific computer system, hence avoiding the ability of malicious software to compromise the license.

Regarding claims 1, 2, and 3: Hashing a file to produce a hash value (Chang Col 7 lines 1-20) a message digest is used to describe the process of hashing the file. Chang states that any known message digest algorithm such as MD2, MD4, or MD5 may be used in the creation of the digest. These algorithms hash the file in the same manner as described by the applicant thus providing for a hash value as the resultant. Encrypting the hash value with a key to generate a signature (Chang Col 7 lines 1-5, Ho Fig 4 paragraph 33-34)

Comparing the generated signature with the original (Chang Fig 6(a, b), Col 9 lines 37-47, Ho Fig 4 paragraph 27) Chang et al states that the file (software) is hashed (i.e. message digest generated). Within the combined system as done within the Ho reference the signature is generated from the unique identifier of the system upon every authentication so as to provide for the functionality of specifying the license for a particular system and performing the integrity check of software as in Chang. File is authenticate if signatures match (Chang Col 9 lines 45-46)

Regarding claims 4-5 and 10: upon verification of the file replacing the first with the second. (Col 8 lines 8-16, 58-59, Col 25 lines 27-56) Chang et al states that the code associated by the signature can take the form of any type of data. As such upon

the authentication of such data it would be necessary to store or act accordingly to the

data type. The execution of pure data in the form of a key for example would only be

feasible for storage or overwriting of pre-existing data as such anticipating the above

claim.

Claims 11-14, 16-17 are a method implementation of the above rejected claims

and as such are rejected upon the same basis.

Claims 6 - 9, 15, and 18 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Chang et al U.S. Patent No. 5,724,425, and Ho et al U.S. Patent

Publication No. 2002/0073325 as applied to claim 1 above, and further in view of

Horstmann U.S. Patent No. 6,044,469.

Regarding claims 6 - 9: Chang et al has taught the method of authentication as

in claim 1 above but fails to teach the implementation of a feature file.

Horstmann, however, teaches the use of such a file to provide for functionality of

subsets of the product.

A plurality of features wherein a subset of the features is activated based upon

the prescribed licensed features. (Horstmann Fig 6, Col 3 lines 39-44, Col 5 lines 54-65)

Horstmann's system of software protection allows for implementation of subsets of a

products full functionality as described.

It would have been obvious to one of ordinary skill in the art at the time of the

applicant's invention to combine the authentication methods of Chang et al with the

functionality of partial licensing as denoted by Horstmann. As it may be seen

(Horstmann Col 2 lines 14-27) one would be motivated to combine these two systems

for added flexibility of ease of configuration of software features and the ability to

maintain security while giving the user further convenience as stated by Horstmann,

thus making this a desirable combination.

Claims 15 and 18 are a method implementation of the above rejected claims and

as such are rejected on the same basis.

(10) Response to Argument

Regarding the Appellant's assertions against the Ho patent, it is the intention of

the Ho reference to show a teaching of an owner key (Ho paragraph 33) that is specific

to the individual system as seen from the recitation of a MAC that is communicated to

the distributor of the software product so that a signature may be provided that is

specifically encoded to that machine with the MAC address (owner key) for the software

product, the key is clearly transferable to an extent necessary to encode the software

prior to being received as indicated within paragraph 33 and figure 4 of the Ho

reference.

The applicant has attempted to characterize the Ho reference as teaching

against the combination, but it clearly provides the same motivation as the Chang

reference of verifying the authenticity of a document against tampering and piracy

(Chang Col 2 lines 44-67, Col 3 lines 1-12, 55-58). As recited by Ho in paragraphs 7

and 11: "...It would be advantageous to devise a protection method that would reduce

the incentive for a potential counterfeiter to counterfeit the system.." and "...a method

and apparatus for protecting the software in a computer system while allowing a user to

make legitimate backup copies of the software."

The Appellant has attempted to characterize one provided embodiment of the Ho

reference as the intended teaching when that is clearly not the case. The appellant on

page 8 of the brief sites Ho paragraph 5 as specifically teaching away from the

Appellant's claims but this recitation occurs within the background of the Ho reference

and is not characterized as the intended situation, wherein a signature file is created

with the owner key, but quite to the contrary paragraph 5 discusses compiling an entire

program specific to each unique system, which is not the teaching of the Ho patent but

an example of previous systems to Ho within the art which the Ho reference explicitly

remedies.

The Appellant further recites that the disclosure of Ho intends for only software

embedded within hardware to be protected by this method but from the immediately

following paragraph of that recitation it is clear that the owner key signature method

disclosed by Ho is intended to protect any software contained within the system (Ho

paragraph 11) as such providing for any type of software and thereby software that is

prospectively received over a network; and further any such deficiency is rectified by

the combination with the Chang reference, wherein Chang clearly teaches receiving

software in such a manner. It should be noted that the applicant at least in independent

claim 1 does not even claim that the software is received over a network, the claim

merely recites "...computer system to receive the software file...".

The Appellant argues on page 9 of 22 of the brief in the last paragraph that the claimed apparatus makes use of a file transmission protocol, but these limitations are not claimed nor are they expressly inherent features of the claims. The Appellant further recites limitations that are shown, as outlined in the above rejection by the Chang reference in view of Ho and does not show how such claim limitations avoid the cited rejection. Chang clearly provides for creating a signature (Chang Col 7 lines 1-20) where from the discussion of Ho at paragraph 33 figure 4 it is clear that the key used to do so is the owner key (MAC address) of the end computer system. Chang further provides for comparing the digital signatures as outlined in figure 6 to verify the authenticity of the software.

In regards to the argument by the Appellant asserting the lack of a case of Prima Facie Obviousness attention is directed to the above statements concerning the specific motivation to protect software against tampering and piracy as outlined by both Chang and Ho. Further all limitations of the claims are taught as seen from the Ho reference at paragraph 33 by the recitation of a MAC address (owner key) that is unique to the specific computer for forming a signature of a software program and Chang further outlining how such communications and reception of the software occurs and compares such signatures.

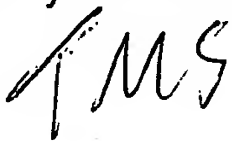All arguments presented by the Appellant are addressed in the above reply.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the

Related Appeals and Interferences section of this examiner's answer.

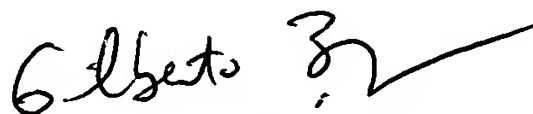For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

TMS

10/12/2006

Conferees:

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Gilberto Barron Jr.

Kambiz Zand